Policy No: 801
Area: Information Technology Services
Adopted: 8/6/2012

Information Security Operational Procedures
Information Security Awareness Policy

POLICY

Educating users and administrators at all levels on the safe and responsible use and handling of information is necessary. The University will facilitate and update a security awareness program for all users of university resources. This awareness program includes web tutorials, computer based training, lectures, and hands on training. The program will be reviewed as necessary or on an annual basis and updated regularly to meet the changing environment of information security.

Each local administrative unit as determined by the Chief Information Officer (CIO), shall develop a written plan to facilitate a local security awareness program specific to the needs of that particular office. A copy of the training plan will be kept on file by the CIO. The plan shall be reviewed as necessary or on an annual basis and updated as needed.

The requirement for an annual review shall be superseded by an incident or information indicating a need for immediate intervention by the local unit or the university as a whole.

Both the University's comprehensive security awareness program and the unit specific program shall be required of all university employees, agents, and affiliates.

GUIDELINES

The University's overall security awareness program shall be broad in scope, addressing at a minimum the following:
• Password policy.
• Electronic communications (chat, email, file sharing, etc.).
• Malicious software.
• Software patches, and anti-virus updates.
• Physical and digital access controls.
• Information handling and disposal.
• Incident response.

• Legislation.
• Consumerism and fraud.

The security awareness program specific to each local administrative unit shall address and focus on the following specific concerns appropriate to their functions:
• Security contact(s).
• Incident response.
• Back-up procedures.
• Electronic communications.
• Business processes.
• Acceptable use.
• Physical and digital security.